**Аннотация**

Целью дипломной работы является разработка механизма прямых трансграничных финансовых операций между цифровыми валютами разных стран.

Дипломный проект выполнен в Microsoft Word 2021, код программы написан средствами текстового редактора PyCharm.

Работа содержит введение, n глав, заключение, библиографический список и приложение.

Данная выпускная квалификационная работа содержит: листов – n, рисунков - n, таблиц - n, формул - n, приложений - n, источников использованной литературы - n.

**Содержание**

[**Определения, обозначения и сокращения** 4](#_Toc165654698)

[**Введение** 7](#_Toc165654699)

[**Глава 1. Анализ предметной области** 10](#_Toc165654700)

[**1.1** **Изучение существующих аналогов блокчейнов** 10](#_Toc165654701)

[**1.2 Анализ потребностей и проблем, которые приложение должно решать** 13](#_Toc165654702)

[**1.2.1 Анализ потенциальных уязвимостей и защита от них** 15](#_Toc165654703)

[**1.3 Выбор среды разработки** 17](#_Toc165654704)

[**1.4 Изучение возможностей фреймворка FastAPI** 19](#_Toc165654705)

[**1.4.1 Преимущества фреймворка FastAPI** 20](#_Toc165654706)

[**1.4.2 Недостатки фреймворка FastAPI** 21](#_Toc165654707)

[**1.5 Выводы по главе 1** 22](#_Toc165654708)

[**Глава 2. Проектирование приложения** 23](#_Toc165654709)

[**2.1 Определение требований к приложению** 23](#_Toc165654710)

[**2.2 Анализ потенциальных уязвимостей** 25](#_Toc165654711)

[**2.3 Разработка структуры приложения и его компонентов** 27](#_Toc165654712)

[**2.4 Разработка интерфейса пользователя** 31](#_Toc165654713)

[**2.5 Описание архитектуры приложения** 33](#_Toc165654714)

[**2.6 Выводы по главе 2** 36](#_Toc165654715)

[**Глава 3. Разработка приложения** 37](#_Toc165654716)

[**3.1 Создание хранилища для блокчейна и его описание** 37](#_Toc165654717)

[**3.2 Реализации логики работы блокчейна** 42](#_Toc165654718)

[**3.2.1 Архитектура** 43](#_Toc165654719)

[**3.2.2 Модуль блокчейна** 48](#_Toc165654720)

[**3.2.3 Модуль ноды** 57](#_Toc165654721)

[**3.2.4 Модуль веб-интерфейса** 62](#_Toc165654722)

# **Определения, обозначения и сокращения**

В настоящей работе применены сокращения и термины с соответствующими определениями.

Блокчейн (с англ. block chain –цепь блоков)  — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих какую-либо информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную [хеш-сумму](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D1%81%D1%83%D0%BC%D0%BC%D0%B0) и хеш-сумму предыдущего блока.

Proof-of-Authority (PoA) (с англ. Доказательство полномочий) — это алгоритм консенсуса, подходящий для частного и разрешенного блокчейна, который опирается на ряд заранее выбранных авторитетных узлов, называемых валидаторами.

Proof-of-Stake (PoS) (с англ. Доказательство владения) — это класс механизмов консенсуса для блокчейнов, которые работают путем выбора валидаторов пропорционально их количеству активов в соответствующей криптовалюте. Это сделано для того, чтобы избежать вычислительных затрат на схемы доказательства работы (POW).

Криптоактивы — это цифровые представления стоимости, основанные на криптографии и децентрализованной одноранговой архитектуре, основанной на технологии распределенного реестра (DLT), которая позволяет двум сторонам напрямую взаимодействовать друг с другом без необходимости в доверенном посреднике.

Фреймворк (с англ. framework – «каркас, структура») – заготовка, готовая модель в IT для быстрой разработки, на основе которой можно дописать собственный код. Он задает структуру, определяет правила и предоставляет необходимый набор инструментов для создания проекта. [1]

ИС – Информационная система.

СУБД (Система управления базами данных) – это инструментальная оболочка пользователя, а ввиду того, что такая среда ориентирована на немедленное удовлетворение запросов пользователя – это всегда система интерпретатор. [2]

HTTP (протокол передачи гипертекста) – это протокол прикладного уровня для Всемирной паутины, составляющий ее самое сердце. HTTP реализуется в двух частях приложений: клиентской и серверной. Клиентская и серверная части программ, исполняемые на различных конечных системах, общаются друг с другом, обмениваясь сообщениями HTTP. Протокол HTTP определяет структуру этих сообщений и порядок обмена между клиентом и сервером. [3]

API (англ. Application Programming Interface – программный интерфейс приложения) – это набор способов и правил, по которым различные программы общаются между собой и обмениваются данными. [4]

SQL (Structured Query Language – язык структурированных запросов) – это язык программирования, который используется для работы с базами данных. [5]

PIP – система управления пакетами, которая используется для установки и управления программными пакетами, написанными на Python.

Форк в блокчейне - это разветвление или разделение цепи блоков на две или более отдельные цепи из-за несогласия в сети по правилам протокола. Это может произойти из-за различий в мнениях участников сети относительно обновлений протокола, конфликтов в консенсусе или атак на сеть. Каждая ветвь может продолжать свое существование, и участники сети должны выбрать, какую ветвь поддерживать.

JSON (JavaScript Object Notation) – это легковесный синтаксис для обмена данными, которые понимают как люди, так и машины. Как следует из названия, JSON основан на скриптовом языке JavaScript; однако, JSON сам по себе полностью не зависим от языка. [6]

Python – мощный компьютерный язык программирования, поддерживающий множество парадигм, который оптимизирован для обеспечения высокой продуктивности программистов, читабельности кода и качества программного обеспечения. [7]

Хеш - результат применения хэш-функции к набору данных, который преобразует входные данные произвольной длины в строку фиксированной длины. Этот хеш является уникальным и практически невозможно восстановить оригинальные данные из него. Хеши используются в криптовалюте для различных целей, таких как создание уникальных идентификаторов для блоков и транзакций, проверка целостности данных, а также обеспечение безопасности и подтверждение подлинности информации. [8]

Дерево Меркла - это структура данных, используемая в криптографии и блокчейне для эффективной проверки целостности и подтверждения содержимого больших объемов данных. Оно строится путем последовательного хэширования пары узлов данных (обычно транзакций) до тех пор, пока не будет получено единое значение, называемое корневым хешем. Этот корневой хеш затем используется для проверки целостности всего дерева: если корневой хеш совпадает, значит, все данные в дереве неизменны и целостны. Деревья Меркла позволяют быстро и эффективно проверять целостность больших объемов данных, что делает их важным элементом в технологиях блокчейна и криптографии.[9]

# **Введение**

В современной эпохе быстрого прогресса в области цифровых технологий и финансовых инноваций наблюдается нарастающая потребность в разработке эффективных механизмов для выполнения трансграничных финансовых операций с использованием различных цифровых валют. Ответом на эту потребность является создание передовых технологических решений, которые обеспечивают высокую степень безопасности, прозрачности и операционной эффективности.

В рамках данной дипломной работы представлен механизм прямых трансграничных финансовых операций между цифровыми валютами разных стран, основанный на технологии блокчейн с использованием протокола Proof of Authority (PoA). Этот механизм является инновационным решением, призванным устранить множество трудностей, связанных с международными финансовыми транзакциями.

Перед детальным изучением разработанного механизма следует уделить внимание историческим предпосылкам. С появлением таких цифровых валют, как Bitcoin и Ethereum, возникла необходимость их применения в международных финансовых операциях. Однако традиционные методы сталкиваются с рядом ограничений, включая вопросы безопасности, время подтверждения транзакций и высокие комиссии.

Применение блокчейн-технологии на основе протокола Proof of Authority (PoA) предлагает решение данных проблем, обеспечивая высокий уровень безопасности и операционной эффективности за счёт включения ограниченного числа доверенных участников для подтверждения транзакций.

Целью данной работы является разработка и реализация механизма прямых трансграничных финансовых операций, который обеспечит высокую надёжность, прозрачность и операционную эффективность с использованием блокчейн-технологии на основе протокола Proof of Authority. Исследование включает анализ требований, проектирование системы, её реализацию и тестирование для гарантии полной функциональности и соответствия заданным критериям.

В конечном итоге, успешное внедрение предложенного механизма способствует углублению международных финансовых отношений, упрощению процессов трансграничных операций и повышению доверия к цифровым валютам как инструменту международных расчётов.

Для успешной реализации системы прямых трансграничных финансовых операций между цифровыми валютами различных стран на базе блокчейн-технологии с применением протокола Proof of Authority (PoA), следует выполнить следующие ключевые задачи:

1. Анализ требований: Идентификация функциональных и нефункциональных требований системы. Это включает обеспечение возможности прямых трансграничных финансовых операций, гарантирование безопасности, минимизация времени подтверждения транзакций, совместимость с разнообразными цифровыми валютами и соответствие нормативным требованиям.

2. Проектирование системы: Разработка комплексной архитектуры системы, выбор подходящих блокчейн-технологий, структурирование сети с особым вниманием к механизмам синхронизации узлов, а также определение интерфейсов для взаимодействия с системой.

3. Реализация синхронизации узлов: Создание механизмов для синхронизации узлов, позволяющих модифицировать код узла и осуществлять асинхронную работу, включая управление собственными ветками блоков.

4. Реализация веб-интерфейса и API: Разработка пользовательского веб-интерфейса для управления аккаунтами, просмотра истории транзакций, а также создание API для интеграции системы с внешними приложениями и сервисами.

5. Генерация адресов транзакций: Разработка системы для генерации уникальных адресов транзакций, что повысит безопасность и гарантирует уникальность каждой операции.

6. Развертывание блокчейн сети: Организация и конфигурация блокчейн сети на основе протокола Proof of Authority, выбор участников сети (доверенных узлов) и настройка параметров сети.

7. Интеграция с внешними системами: Разработка интерфейсов для взаимодействия с внешними системами, такими как цифровые кошельки, криптовалютные биржи и финансовые учреждения.

8. Тестирование и оптимизация: Проведение всестороннего тестирования системы для проверки соответствия требованиям, исправление выявленных ошибок и оптимизация производительности и безопасности.

9. Запуск и поддержка: Внедрение системы в эксплуатацию, обеспечение ее стабильной и непрерывной работы, включая мониторинг производительности, обновление ПО и реагирование на технические проблемы.

Эти задачи, учитывая специфику цифровых валют и международных финансовых операций, обеспечат создание эффективной, безопасной и надежной системы для проведения прямых трансграничных финансовых операций на основе блокчейн-технологии.

# **Глава 1. Анализ предметной области**

## **Изучение существующих аналогов блокчейнов**

При анализе текущих блокчейн-систем и их механизмов консенсуса можно выявить ряд важных аспектов. Давайте рассмотрим ключевые характеристики некоторых из них:

Bitcoin (Proof of Work):

- Механизм консенсуса: Proof of Work (PoW) требует от майнеров решения вычислительно сложных задач для генерации новых блоков и подтверждения транзакций.

- Недостатки: Высокое энергопотребление, замедление скорости подтверждения транзакций, потенциальная централизация майнинга крупными игроками.

Ethereum (Переход к Proof of Stake):

- Механизм консенсуса: Ethereum в настоящее время использует PoW, но планирует перейти на Proof of Stake (PoS), где верификация транзакций осуществляется участниками, пропорционально их доле валюты в сети.

- Недостатки: В текущем состоянии Ethereum сталкивается с теми же проблемами, что и Bitcoin. В перспективе PoS может привести к концентрации криптовалюты в руках небольшой группы участников.

Ripple (Протокол консенсуса):

- Механизм консенсуса: Ripple использует уникальный протокол консенсуса, который позволяет достигать согласия по транзакциям без необходимости в вычислительных задачах.

- Недостатки: Система зависит от доверия к центральной организации, управляющей списком узлов, участвующих в процессе консенсуса.

Cardano (Ouroboros Proof of Stake):

Преимущества: Энергоэффективный протокол PoS, строгий академический подход к разработке и высокий уровень безопасности.

Недостатки: Относительно новая платформа, которая еще не достигла уровня распространения Ethereum или Bitcoin.

Hyperledger Fabric (Permissioned Blockchain):

Преимущества: Высокий уровень контроля и безопасности, способность к эффективной масштабируемости в корпоративных приложениях.

Недостатки: Отсутствие децентрализации, что может не соответствовать требованиям проектов, предполагающих широкое участие неконтролируемого числа узлов.

Tezos (On-chain Governance):

Преимущества: Механизмы управления, позволяющие автоматически обновлять протокол без хард-форков.

Недостатки: Сложности, связанные с принятием изменений всеми участниками сети, могут замедлить процесс развития платформы.

Теперь рассмотрим, почему механизм консенсуса Proof of Authority (PoA) является предпочтительным для трансграничных финансовых операций:

- Эффективность и скорость: PoA обеспечивает быструю верификацию транзакций за счет использования доверенных узлов, что критически важно для операций в реальном времени.

- Низкая стоимость транзакций: PoA исключает необходимость в значительных вычислительных ресурсах, снижая стоимость транзакций по сравнению с PoW и PoS.

- Высокий уровень безопасности: При адекватной настройке и управлении списком доверенных узлов, PoA может обеспечить высокую защиту от атак.

- Гибкость и управляемость: PoA позволяет гибко управлять списком узлов, адаптируя сеть под специфические требования трансграничных операций.

Кроме того, блокчейн на базе PoA не требует использования nonce, что необходимо в PoW для генерации блоков. Это исключает ненужные вычисления, позволяя снизить энергопотребление и повысить общую производительность системы. Важно отметить, что PoW подвержен риску 51% атаки, в то время как PoA, благодаря своей структуре и механизмам защиты, значительно менее уязвим к внешним угрозам. В случае попытки взлома одной из узлов, происходит форк сети, и узлы автоматически рассинхронизируются, что предотвращает возможные внешние взломы.

Таким образом, Proof of Authority представляет собой оптимальное решение для системы трансграничных транзакций, обеспечивая высокую скорость обработки, низкую стоимость, повышенную безопасность и удобство управления.

## **1.2 Анализ потребностей и проблем, которые приложение должно решать**

Данное приложение призвано решать ключевые вызовы в сфере международных финансовых операций. Основная проблема, на решение которой направлено приложение, — неэффективность и высокая стоимость традиционных методов международных платежей. Существующие системы часто обременены высокими комиссиями и длительными сроками обработки транзакций, что затрудняет оперативное и экономически выгодное выполнение трансграничных платежей.

Проблема недостаточной прозрачности и безопасности также стоит на повестке дня. В классических финансовых системах отсутствует должный уровень прозрачности операций и защиты данных, что порождает риски и недоверие среди участников финансовых операций.

Кроме того, существует проблема затяжного и обременительного процесса соблюдения регуляторных требований в рамках международных транзакций. Традиционные системы требуют многочисленных проверок и документации для соответствия регуляторным нормам, что увеличивает время обработки транзакций и ведет к дополнительным издержкам.

Таким образом, приложение должно обеспечивать:

- Снижение комиссий и минимизацию задержек в международных платежах;

- Повышение прозрачности и безопасности операций;

- Упрощение процесса соблюдения регуляторных требований.

Отдельное внимание заслуживает обеспечение доверия к узлам блокчейна при отсутствии механизма Proof of Work. Предлагается механизм, позволяющий каждому владельцу ноды модифицировать свой код таким образом, что при изменениях нода автоматически перестанет синхронизироваться с остальной частью сети, исключая риски недобросовестного поведения и повышая надежность системы.

Для успешной интеграции и функционирования блокчейна на территории России необходимо учесть соответствие местному законодательству, особенно в части требований KYC и анти-отмывания денег. Интеграция с уже существующими информационными системами и сервисами окажет существенное влияние на снижение "трения" при внедрении и повышение общей эффективности использования приложения.

Рассмотрение экономической целесообразности применения блокчейна на базе PoA включает анализ рыночной конкуренции, развитие информационных технологий и потенциальные санкции, что может стимулировать широкое принятие данной технологии как альтернативного решения для обхода ограничений и улучшения финансовых операций на международном уровне.

### **1.2.1 Анализ потенциальных уязвимостей и защита от них**

Анализ потенциальных уязвимостей и защита от них играет ключевую роль в обеспечении безопасности и надежности блокчейна на основе Proof of Authority (PoA) для проведения трансграничных транзакций. В этой главе проводится детальный анализ потенциальных уязвимостей блокчейна и рассматриваются методы и меры для их предотвращения.

Основные уязвимости и меры защиты:

1. Атака 51%:

- Описание: В традиционных блокчейнах, таких как Bitcoin, атака 51% происходит, когда один участник или группа участников контролирует более половины вычислительной мощности сети, что позволяет им манипулировать подтверждением транзакций.

- Меры защиты в PoA: В блокчейне на основе PoA, где доверие основано на предварительно утвержденном списке валидаторов, риск такой атаки существенно снижен. Вместе с тем, чтобы минимизировать риски, необходимо тщательное управление и регулярная проверка списка валидаторов, а также внедрение механизмов для автоматической рассинхронизации с сомнительными узлами.

2. Вредоносные атаки на смарт-контракты:

- Описание: Смарт-контракты могут содержать уязвимости в коде, которые могут быть эксплуатированы для манипулирования выполнением контракта или кражи средств.

- Меры защиты: Реализация многоуровневого процесса аудита кода смарт-контрактов, включая автоматические инструменты проверки и ручной аудит экспертами, а также механизмы быстрого отката транзакций в случае обнаружения аномалий.

3. DDoS-атаки (Distributed Denial of Service):

- Описание: Злоумышленники могут направить чрезмерное количество трафика на сеть, что приведет к перегрузке и невозможности обработки легитимных запросов.

- Меры защиты: Использование распределенной архитектуры сети, методов ограничения скорости запросов, а также применение специализированных сетевых решений для защиты от DDoS-атак.

Дополнительные меры защиты:

- Шифрование данных: Необходимо использовать современные алгоритмы шифрования для защиты данных, передаваемых в сети, и хранящихся в блокчейне, включая личные ключи и информацию о транзакциях.

- Механизмы аутентификации и авторизации: Внедрение многофакторной аутентификации и строгих политик доступа для обеспечения того, чтобы только авторизованные пользователи могли выполнять операции.

- Аудит и мониторинг\* Разработка систем аудита и мониторинга для отслеживания активности в сети и оперативного реагирования на подозрительные действия.

- Регулярные обновления и патчи: Обеспечение своевременного обновления программного обеспечения и аппаратных компонентов для устранения известных уязвимостей.

- Обучение пользователей: Проведение регулярных тренингов для пользователей с целью повышения осведомленности о потенциальных угрозах и методах их предотвращения.

Эффективная реализация этих мер предосторожности способна обеспечить высокий уровень безопасности и надежности блокчейн-системы на основе PoA, устраняя основные уязвимости и предотвращая потенциальные атаки.

## **1.3 Выбор среды разработки**

Выбор среды разработки является критически важным этапом в разработке любой технологии, включая блокчейн. Причины выбора Python для данного проекта обусловлены несколькими ключевыми факторами, которые делают его особенно подходящим для разработки сложных систем, таких как блокчейн:

1. Простота и читаемость кода: Python известен своим чистым и легко читаемым синтаксисом, что упрощает разработку, отладку и последующее обслуживание кода. Это особенно важно в проектах, где участвует множество разработчиков и требуется поддержка и обновление кода.

2. Богатая экосистема: Python поддерживается обширной библиотекой библиотек и фреймворков, которые могут значительно ускорить разработку и предоставляют инструменты для почти любой задачи — от веб-разработки до работы с базами данных и машинным обучением.

3. Универсальность: Python поддерживается на всех основных платформах, что делает его универсальным выбором для разработки приложений, которые должны работать в различных средах.

4. Поддержка асинхронности и многопоточности: Python обладает отличной поддержкой асинхронного и многопоточного программирования, что критически важно для высокопроизводительных приложений, таких как транзакционные системы на блокчейне.

5. Активное сообщество: Наличие широкого и активного сообщества Python обеспечивает доступ к обширной базе знаний, форумам поддержки и обучающим материалам, что значительно упрощает решение возникающих проблем и ускоряет процесс разработки.

Сравнение фреймворков FastAPI и Flask

Для разработки веб-интерфейса к блокчейну были рассмотрены два популярных Python фреймворка — FastAPI и Flask. Вот краткое сравнение их основных характеристик:

- FastAPI:

- Производительность: Благодаря асинхронному программированию FastAPI предлагает высокую производительность.

- Типизация данных и валидация: FastAPI поддерживает автоматическую валидацию данных и предоставляет возможности современной типизации Python, что улучшает безопасность и надежность приложения.

- Документация: FastAPI автоматически генерирует документацию, что упрощает разработку и поддержку API.

- Поддержка стандартов OpenAPI и Swagger: Это облегчает интеграцию и использование в различных средах.

- Flask:

- Гибкость: Flask предлагает большую гибкость и простоту для разработки простых веб-приложений.

- Меньшая поддержка асинхронности: Flask имеет ограниченную поддержку асинхронного программирования по сравнению с FastAPI.

Исходя из анализа, FastAPI является предпочтительным выбором для данного проекта блокчейна из-за его высокой производительности, поддержки асинхронности и улучшенной безопасности, что особенно важно для систем, обрабатывающих транзакции и финансовые данные.

## **1.4 Изучение возможностей фреймворка FastAPI**

FastAPI — это современный и эффективный веб-фреймворк на языке Python, который предоставляет разработчикам мощные инструменты для создания веб-приложений. Он позволяет быстро и легко разрабатывать API, обеспечивая высокую производительность за счет использования современных технологий.

Для разработки веб интерфейса к блокчнейну FastAPI может быть отличным выбором, так как он обладает рядом полезных возможностей. Например, благодаря асинхронной поддержке можно создать быстродействующие веб-приложение, способное обрабатывать большое количество запросов одновременно. Кроме того, FastAPI предоставляет интуитивный и простой в использовании интерфейс для описания схем данных API с помощью Pydantic, что облегчает разработку и поддержку кода.

Еще одним преимуществом FastAPI является возможность автоматической генерации документации API на основе аннотаций в коде, что значительно упрощает процесс документирования вашего приложения. Кроме того, FastAPI обладает встроенной поддержкой валидации данных, автоматической сериализации и десериализации запросов и многими другими полезными функциями.

Использование FastAPI для блокчейн-приложения позволит не только создать эффективное и надежное веб-приложение, но и изучить современные подходы к разработке API, работе с асинхронным кодом и использованию современных технологий веб-разработки.

### **1.4.1 Преимущества фреймворка FastAPI**

Одним из ключевых достоинств FastAPI является его высокая производительность. Благодаря применению современных технологий асинхронного программирования, данный фреймворк обеспечивает высокую скорость работы и эффективное использование ресурсов, что делает его отличным выбором для создания высоконагруженных веб-приложений.

Кроме того, FastAPI предлагает удобный и интуитивно понятный интерфейс для разработчиков. Он использует аннотации Python для описания эндпоинтов и схем данных API, что делает процесс создания веб-приложений более простым и эффективным. Благодаря автоматической генерации интерактивной документации на основе аннотаций в коде, разработчики могут быстро и легко создавать, и поддерживать документацию без дополнительных усилий.

Еще одним преимуществом FastAPI является встроенная поддержка валидации данных, что обеспечивает безопасность API и помогает избежать ошибок ввода. Благодаря поддержке различных форматов данных, таких как JSON, формы HTML, файлы и другие, FastAPI является универсальным инструментом для разработки разнообразных веб-приложений, обеспечивая разработчикам широкие возможности при создании функциональных и эффективных веб-сервисов.

### **1.4.2 Недостатки фреймворка FastAPI**

FastAPI, несмотря на свои многочисленные достоинства, также имеет некоторые недостатки. В частности, такой фреймворк может показаться избыточным для небольших проектов или приложений, требующих минималистического подхода. Кроме того, изучение особенностей и функционала FastAPI может потребовать времени и усилий, особенно для начинающих программистов, не знакомых с асинхронным программированием или аннотациями в Python.

Еще одним недостатком FastAPI является отсутствие широкого сообщества и большого количества сторонних библиотек и плагинов, как у более узнаваемых и распространенных фреймворков. Это может затруднить поддержку и развитие проекта в долгосрочной перспективе, особенно если возникнет необходимость в специфической функциональности, которая не предусмотрена по умолчанию в FastAPI.

Кроме того, из-за своей особенности использования асинхронного программирования FastAPI может создавать некоторые сложности в проектировании архитектуры приложения. Это может потребовать дополнительных усилий и времени для овладения соответствующими концепциями и методиками разработки, что также считается недостатком данного фреймворка.

## **1.5 Выводы по главе 1**

Я рассмотрел различные аспекты разработки блокчейна на основе механизма Proof of Authority (PoA) для системы трансграничных транзакций. Проведенный анализ выявил, что такой блокчейн способен эффективно решать ряд ключевых проблем, среди которых - высокие комиссии и задержки в международных платежах, неэффективность традиционных финансовых систем, недостаточная прозрачность и безопасность операций, а также сложности соблюдения регуляторных требований.

Изучение существующих аналогов блокчейнов позволило выявить различные механизмы консенсуса, такие как Proof of Work (PoW), Proof of Stake (PoS) и Consensus Protocol. Однако, по результатам анализа, было установлено, что механизм PoA представляет собой наиболее подходящий вариант для решения задач системы трансграничных транзакций, благодаря своей эффективности, низкой стоимости проведения транзакций, высокому уровню безопасности и гибкости управления.

Кроме того, в рамках анализа были выявлены дополнительные особенности предлагаемой системы, такие как возможность изменения кода узлов и автоматическая рассинхронизация сети в случае попытки взлома, что дополнительно повышает ее безопасность и надежность.

Таким образом, на основании проведенного анализа можно сделать вывод о целесообразности и перспективности использования блокчейна на основе механизма PoA для реализации системы трансграничных финансовых операций.

# **Глава 2. Проектирование приложения**

## **2.1 Определение требований к приложению**

Определение требований к приложению блокчейна на основе механизма Proof of Authority (PoA) для проведения трансграничных транзакций включает в себя ряд ключевых аспектов, которые необходимо учесть для успешной разработки и функционирования системы. Эти требования включают в себя:

1. Эффективность трансграничных платежей: Приложение должно обеспечивать быструю и надежную передачу средств между участниками из разных стран с минимальными комиссиями и задержками.
2. Прозрачность и безопасность операций: Система должна обеспечивать высокий уровень прозрачности и безопасности всех транзакций, чтобы участники могли доверять целостности и результатам проведенных операций.
3. Соответствие регуляторным требованиям: Приложение должно быть способно соблюдать регуляторные нормы и требования, действующие в различных странах, чтобы предотвратить возможные конфликты и проблемы с законодательством.
4. Гибкость и масштабируемость: Система должна быть гибкой и легко масштабируемой, чтобы адаптироваться к изменяющимся потребностям рынка и обеспечивать возможность обработки большого объема транзакций.
5. Управление доступом и безопасность: Приложение должно обеспечивать строгий контроль доступа к системе и конфиденциальность информации, защищая данные пользователей от несанкционированного доступа и взлома.
6. Легкость использования и интеграции: Система должна быть удобной в использовании как для конечных пользователей, так и для предприятий, а также легко интегрироваться с существующими финансовыми и технологическими системами.
7. Автоматизация процессов: Приложение должно обеспечивать автоматизацию ключевых процессов, связанных с проведением трансграничных транзакций, чтобы уменьшить ручную работу и повысить эффективность операций.

Учитывая эти требования, разработка и реализация приложения блокчейна на основе механизма PoA должны быть направлены на обеспечение высокого качества обслуживания и удовлетворение потребностей всех заинтересованных сторон.

## **2.2 Анализ потенциальных уязвимостей**

Создание такого блокчейна требует отслеживания и устранения уязвимостей.

Примеры:

1. Уязвимости в программном обеспечении (ПО):

- Уязвимости в смарт-контрактах: Недавние инциденты показали, что смарт-контракты могут содержать ошибки, которые могут привести к утрате средств или даже к полной уязвимости системы блокчейна. Примером является уязвимость "Reentrancy", когда атакующая сторона многократно вызывает внешние контракты перед завершением выполнения основного контракта. Проверка смарт-контрактов на уязвимости и использование проверенных шаблонов контрактов может помочь предотвратить такие атаки.

2. Уязвимости операционной системы (ОС):

- Атаки на уровне операционной системы: Вредоносные программы, такие как вредоносные скрипты, руткиты и т. д., могут использоваться для компрометации узлов блокчейна и веб-приложений. Важно регулярно обновлять операционные системы, использовать антивирусное программное обеспечение и следить за активностью на серверах для предотвращения таких атак.

3. Уязвимости веб-приложений:

- Атаки на сторону клиента (Client-Side Attacks): XSS (межсайтовый скриптинг), CSRF (межсайтовая подделка запросов), а также атаки на сторону клиента могут быть использованы для компрометации веб-приложений, включая те, которые взаимодействуют с блокчейном. Для предотвращения таких атак важно использовать санкционированные методы аутентификации и авторизации, а также правильно настраивать заголовки безопасности HTTP.

4. Методы сертификации:

- SSL/TLS сертификаты: Веб-приложения, особенно те, которые взаимодействуют с блокчейном и содержат чувствительные данные, должны использовать SSL/TLS сертификаты для обеспечения шифрования трафика и проверки подлинности. Важно правильно настроить серверы, чтобы избежать возможных уязвимостей, связанных с неправильной конфигурацией SSL/TLS.

5. Валидаторы и ноды:

- DDoS атаки на узлы: Ноды блокчейна и валидаторы могут стать целью DDoS-атак, что приведет к отказу в обслуживании и потере доступности для других участников сети. Для предотвращения таких атак можно использовать средства защиты от DDoS, такие как фильтрация трафика и распределенные системы защиты.

6. Избежание ошибок 0 дня:

- Регулярное обновление: Один из наиболее важных методов предотвращения ошибок 0 дня - это регулярное обновление программного обеспечения, включая операционные системы, приложения и зависимости. Постоянное отслеживание уязвимостей и применение патчей является необходимым.

## **2.3 Разработка структуры приложения и его компонентов**

Основные компоненты приложения и их взаимосвязи:

1. Chain:

- Описание: Этот компонент содержит базу данных блоков и транзакций. Здесь осуществляется генерация мнемоник, создание и проверка подписей, а также получение и создание транзакций и блоков.

- Взаимосвязь с другими компонентами: Chain взаимодействует с компонентом Crypto для шифрования мнемонических фраз и выполнения математических операций, необходимых для создания и проверки подписей. Также Chain обеспечивает данные, которые могут быть использованы Node для проверки и добавления новых блоков в цепочку.

2. Crypto:

- Описание: Этот модуль отвечает за создание транзакций, составление транзакций и компоновку байтов, а также за шифрование мнемонических фраз и выполнение математических операций.

- Взаимосвязь с другими компонентами: Crypto используется Chain для создания и проверки подписей транзакций, а также для шифрования мнемонических фраз. Кроме того, он может взаимодействовать с Node для создания новых транзакций и блоков.

3. Node:

- Описание: Этот модуль представляет собой ноду блокчейна, которая выпускает и валидирует блоки. У ноды есть свой API, который используется другими компонентами приложения.

- Взаимосвязь с другими компонентами: Node использует данные из Chain для проверки целостности блоков и транзакций, а также может использовать Crypto для создания новых блоков. Его API доступен компоненту Web для взаимодействия с пользователем.

4. Web (Веб-интерфейс):

- Описание: Этот модуль предоставляет графический интерфейс пользователям через веб-сайт. Включает в себя HTML и JS скрипты для взаимодействия с пользователем.

- Взаимосвязь с другими компонентами: Web взаимодействует с Node через его API для получения данных о блоках и транзакциях, а также для отправки новых транзакций.

Каждый из этих компонентов играет ключевую роль в функционировании приложения, а их взаимосвязь обеспечивает согласованную работу системы в целом.

Chain служит основным хранилищем данных блокчейна, предоставляя информацию о блоках и транзакциях для других компонентов. Crypto обеспечивает безопасность и целостность данных благодаря криптографическим методам, а также осуществляет создание и проверку транзакций. Node является ядром сети, отвечая за создание новых блоков и проверку их на валидность, а также предоставляет API для взаимодействия с другими компонентами. Web обеспечивает пользовательский интерфейс, позволяя пользователям взаимодействовать с блокчейном через веб-интерфейс.

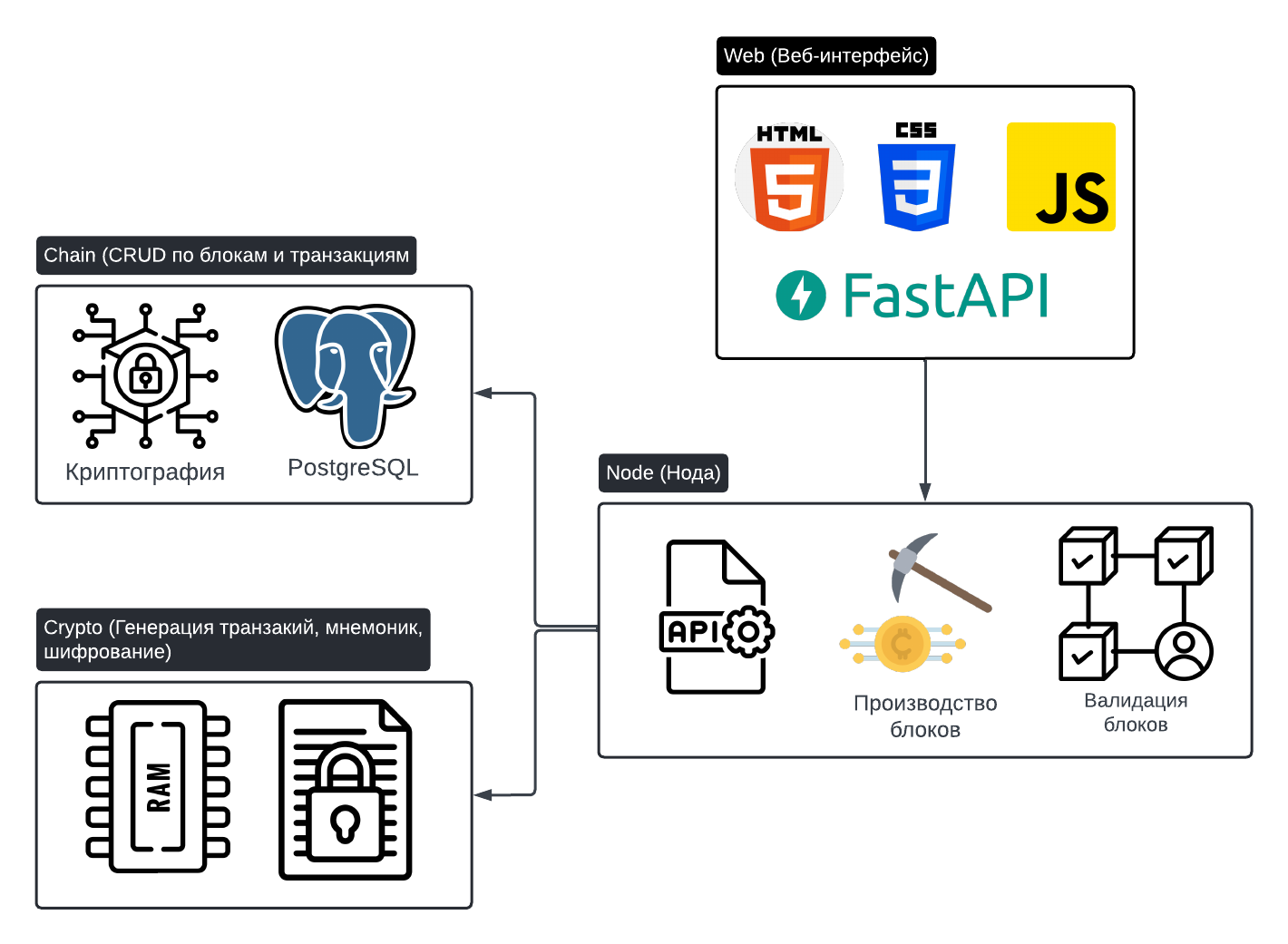


Рисунок 1 – архитектура модулей

Таким образом, компоненты взаимодействуют между собой, обмениваясь данными и обеспечивая работоспособность и эффективность всей системы блокчейна на механизме PoA для проведения трансграничных транзакций.

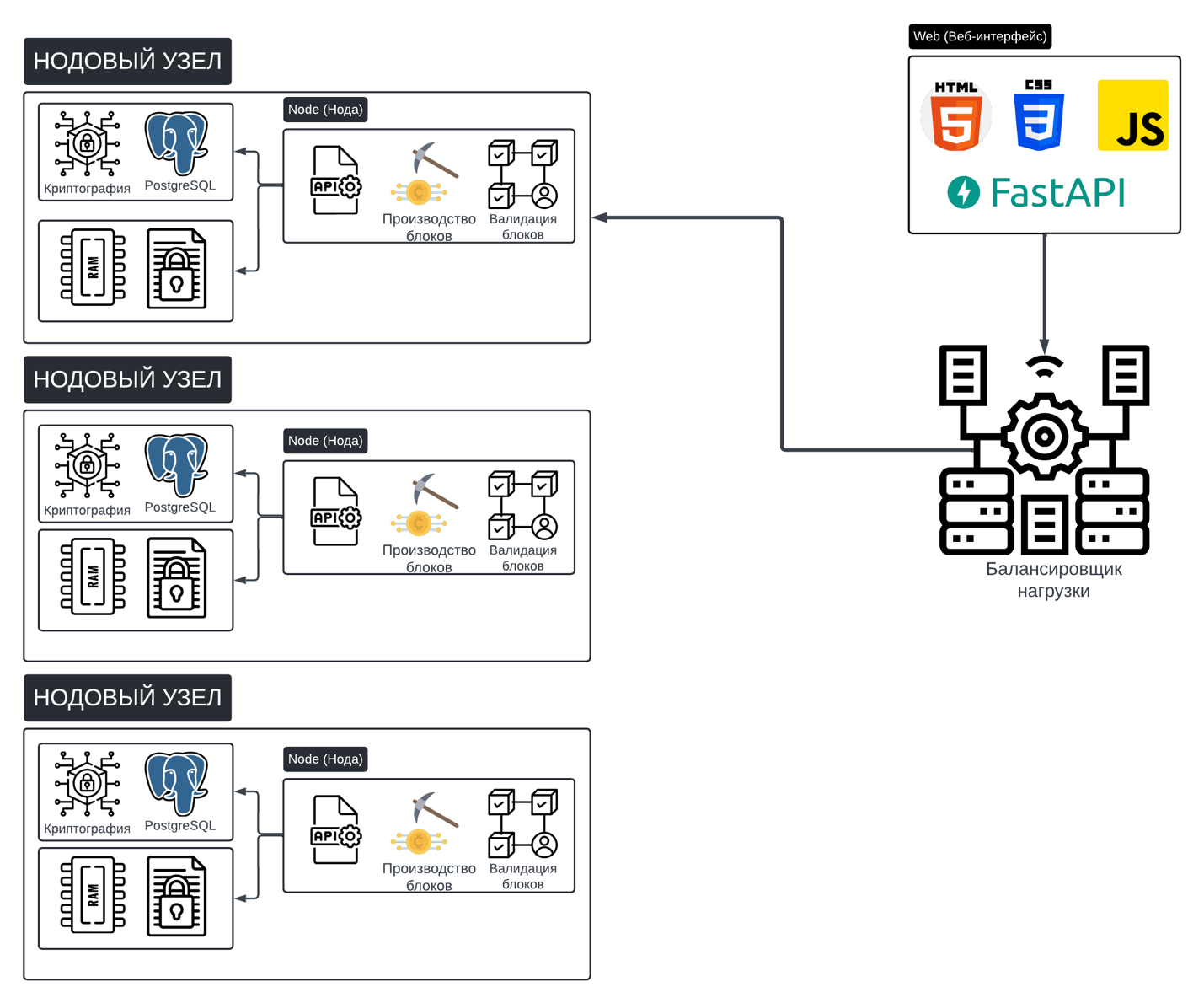


Рисунок 2 – архитектура модулей с балансировщиком

## **2.4 Разработка интерфейса пользователя**

В данном разделе рассмотрена разработка интерфейса пользователя для веб версии блокчейна на PoA.

Для разработки интерфейса пользователя блокчейн-приложения с учетом предложенных компонентов следует уделить особое внимание каждому из них.

1. Окно аутентификации:

- Форма ввода мнемоники для аутентификации пользователя.

- Возможность генерации мнемоники для нового пользователя.

2. Кошелек:

- Отображение баланса пользователя и его адрес в удобном для восприятия виде.

- Вкладки для отправки криптовалюты и создания подписей, где пользователь сможет вводить необходимые данные для совершения операции.

- Вкладки для просмотра транзакций, где отображаются все отправленные и полученные транзакции пользователя с возможностью сортировки и фильтрации.

3. Окно просмотра транзакций:

- Отображение детальной информации о каждой транзакции, включая ее характеристики и данные блока, в котором она была включена.

- Возможнлсть просмотра связанных транзакций для лучшего понимания контекста операции.

4. Окно просмотра блока:

- Отображение всех данных блока, включая список транзакций, включенных в него.

- Возможность просмотра подробной информации о каждой транзакции в блоке.

5. Окно обзорщика блоков:

- Визуализированный процесс генерации блоков в реальном времени.

- Поиск конкретного блока по его номеру или транзакции по ее хешу для быстрого доступа к нужной информации.

Помимо этого, обеспена плавная навигация между различными окнами и возможность быстрого доступа к основной функциональности приложения. Уделено внимание дизайну интерфейса, он сделан его интуитивно понятным и привлекательным для пользователя.

## **2.5 Описание архитектуры приложения**

Архитектура приложения для системы трансграничных транзакций в виде блокчейна на механизме Proof of Authority (PoA) включает в себя следующие компоненты:

1. Клиентский веб-интерфейс:

- Веб-приложение, которое предоставляет пользовательский интерфейс для взаимодействия с блокчейном.

- Реализует функциональность аутентификации пользователей, просмотра баланса и истории транзакций, отправки транзакций и просмотра информации о блоках.

- Использует HTML, CSS и JavaScript для создания пользовательского интерфейса и взаимодействия с API нод.

2. Субд Postgresql:

- Система управления базами данных, используемая для хранения информации о блоках, транзакциях и других данных блокчейна.

- Хранит информацию о пользовательских аккаунтах, балансах, истории транзакций и другие сведения, необходимые для функционирования приложения.

3. Ноды:

- Узлы блокчейна, отвечающие за создание, проверку и хранение блоков.

- Каждая нода в сети обрабатывает транзакции, создает новые блоки и участвует в процессе достижения консенсуса.

- Ноды взаимодействуют между собой для распространения блоков и поддержания целостности сети.

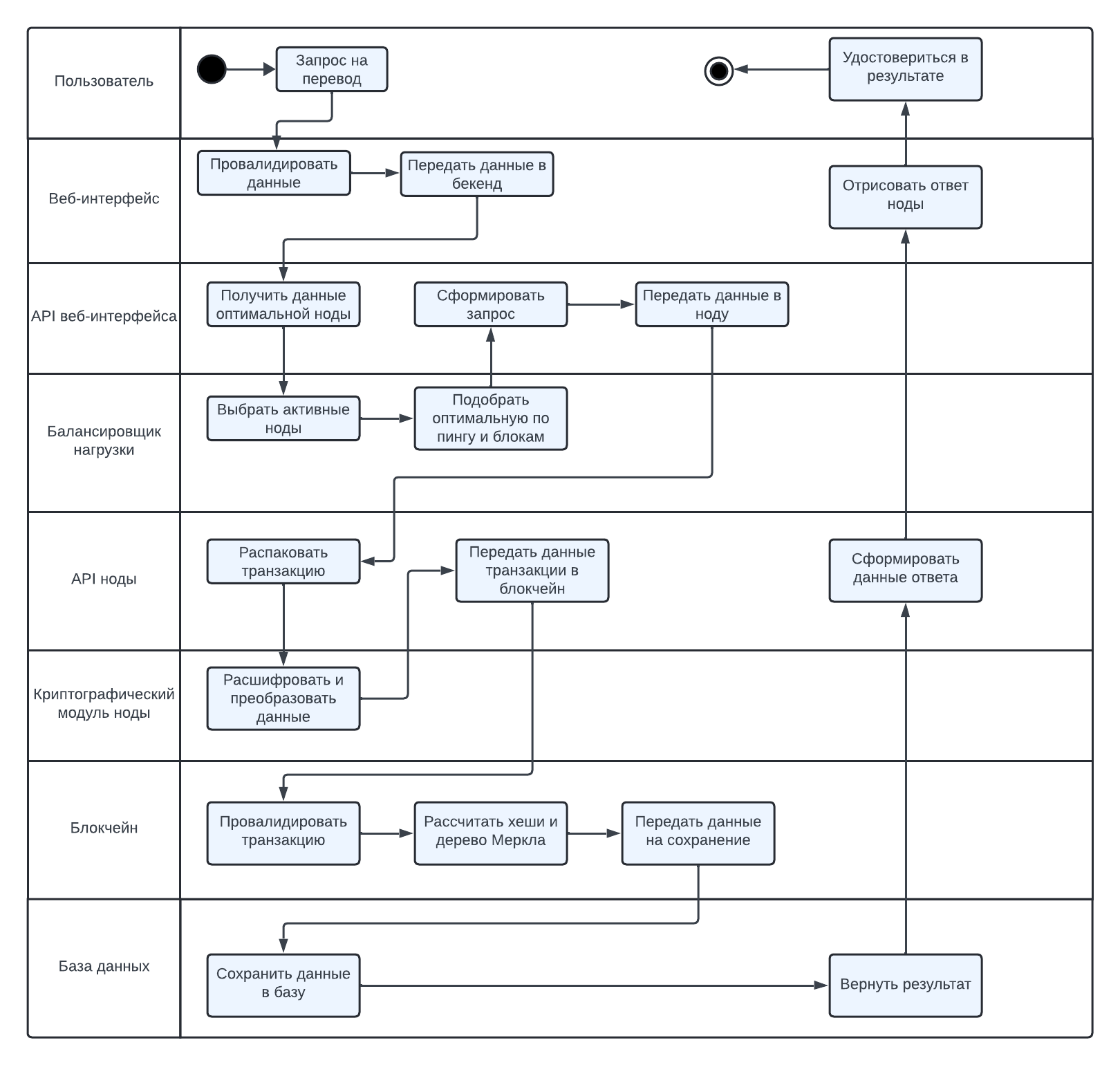


Рисунок 3 – Путь запроса по архитектуре

Архитектура приложения предполагает, что клиентский веб-интерфейс взаимодействует с нодами блокчейна через их API для получения информации о блоках, транзакциях и выполнения операций с аккаунтами. Ноды в свою очередь взаимодействуют друг с другом для распространения блоков и поддержания актуального состояния блокчейна. Данные о блоках, транзакциях и аккаунтах хранятся в базе данных Postgresql для обеспечения удобного доступа и быстрой обработки информации.

## **2.6 Выводы по главе 2**

Анализируя вышеописанные модули и архитектуру приложения, можно сделать следующие выводы.

Клиентский веб-интерфейс играет ключевую роль в обеспечении пользовательского опыта. Он предоставляет удобный доступ к функционалу блокчейна, включая просмотр информации о транзакциях и блоках, а также выполнение операций с аккаунтами.

Использование системы управления базами данных Postgresql обеспечивает надежное хранение данных блокчейна и обеспечивает быстрый доступ к ним. Это важно для обеспечения эффективной работы приложения и обеспечения целостности данных.

Ноды блокчейна играют ключевую роль в обеспечении безопасности и целостности сети. Механизм PoA обеспечивает высокую эффективность и надежность работы нод, что является важным аспектом для системы трансграничных транзакций.

В целом, архитектура приложения объединяет эти компоненты в единую систему, обеспечивая высокий уровень безопасности, прозрачности и эффективности для пользователей.

# **Глава 3. Разработка приложения**

## **3.1 Создание хранилища для блокчейна и его описание**

В данной главе проводем анализ различных видов хранилищ данных и их применимости для блокчейна на механизме Proof of Authority (PoA). В этой главе сравним следующие виды хранилищ:

1. Реляционные базы данных:

- Примеры: PostgreSQL, MySQL, Oracle.

- Плюсы: Обеспечивают структурированное хранение данных с возможностью использования сложных запросов. Обеспечивают надежность и целостность данных.

- Минусы: Могут быть менее масштабируемыми по сравнению с NoSQL базами данных. Требуют более тщательного проектирования схемы данных.

2. NoSQL базы данных

- Примеры: MongoDB, Cassandra, Redis.

- Плюсы: Обеспечивают гибкое хранение данных без жесткой схемы. Обладают высокой масштабируемостью и способностью обрабатывать большие объемы данных.

- Минусы: Могут быть менее эффективными при выполнении сложных запросов, требуют дополнительной работы по обеспечению согласованности данных.

3. Файловые системы:

- Примеры: Amazon S3, Google Cloud Storage, IPFS.

- Плюсы: Простота использования, низкая стоимость хранения данных. Поддерживают различные типы данных, включая файлы и документы.

- Минусы: Могут быть менее эффективными при выполнении операций поиска и обработки данных. Могут не обеспечивать такой же уровень надежности и безопасности, как реляционные базы данных.

PostgreSQL является мощной реляционной базой данных, которая обладает рядом характеристик, делающих ее подходящим выбором для использования в блокчейне на механизме Proof of Authority (PoA):

1. Структурированное хранение данных: PostgreSQL позволяет организовать данные в виде таблиц с жесткой схемой, что особенно полезно для блокчейна, где необходимо хранить информацию о блоках, транзакциях, аккаунтах и других аспектах сети.

2. Транзакционная безопасность: PostgreSQL обеспечивает ACID-свойства транзакций (Atomicity, Consistency, Isolation, Durability), что гарантирует целостность данных и надежность операций в блокчейне. Это особенно важно для обеспечения согласованности данных в децентрализованной среде.

3. Поддержка сложных запросов: PostgreSQL предоставляет широкие возможности для выполнения сложных запросов и аналитики данных. Это позволяет эффективно работать с большим объемом информации, характерным для блокчейна.

4. Масштабируемость: PostgreSQL обладает возможностью масштабироваться как вертикально (путем увеличения ресурсов сервера), так и горизонтально (путем использования репликации и шардинга). Это позволяет блокчейну на PoA обрабатывать большие объемы данных и поддерживать высокую производительность.

5. Большое сообщество и поддержка: PostgreSQL является одной из самых популярных открытых реляционных баз данных, что обеспечивает широкую поддержку, обновления и интеграцию с другими инструментами и технологиями.

6. Открытый исходный код: PostgreSQL распространяется под лицензией открытого исходного кода, что делает его доступным для использования без затрат на лицензирование и обеспечивает прозрачность разработки и независимость от поставщика.

Все эти факторы делают PostgreSQL привлекательным выбором для хранения данных в блокчейне на PoA, обеспечивая надежность, производительность и гибкость в работе с данными.

Перейдем к описанию структуры базы данных. База данных будет состоять из нескольких таблиц, каждая из которых будет хранить определенный тип данных. Рассмотрим каждую таблицу подробнее.

1. Таблица «block»

Эта таблица содержит в себе цепочку блоков. Состоит из следующих полей:

- id: Первичный уникальный ключ блока.

- block\_number: Числовой уникальный номер блока начиная с genesis блока

- block\_hash: Хеш блока, созданный на основе его атрибутов (номера блока, дерева меркла, предыдущего блока, времени итд) (текстовый формат)

- previous\_hash: Хеш предыдущего блока (текстовый формат)

- merkle\_root: Дерево меркла блока, построенное на основе последовательного хеширования транзакций блока, может быть null если транзакций в блоке нет (текстовый формат)

- authority\_id: Опознавательный ключ ноды валидатора которая выпустила данный блок (текстовый формат)

- timestamp: Дата выпуска блока в микросекундах

1. Таблица «transaction»

- id: Первичный уникальный ключ транзакции.

- sender\_address: Адрес отправителя транзакции (текстовый формат)

- recipient\_address: Адрес получателя транзакции (текстовый формат)

- amount: Числовая сумма отправленных активов. Хранится в базе в целочисленном виде, отображается с точностью 2 знака только визуально.

- timestamp: Дата совершения транзакции в микросекундах

- transaction\_hash: Хеш транзакции составленный на основе ее данных (отправителя, получателя, суммы, времени)

- block\_id: Ключ связанного блока в базе данных

- block\_number: Номер блока. После подтверждения транзакции она попадает в блок, а после подтверждения блока в это поле вписывается его номер.

После проектирования структуры базы данных для блокчейна необходимо приступить к созданию таблиц. Для этого используется язык SQL, который позволяет определить имена таблиц, их атрибуты и типы данных. Каждая таблица также должна иметь первичные ключи, индексы и ограничения в соответствии с требованиями. Этот процесс осуществляется с помощью SQL-инструкций CREATE TABLE.

После создания таблиц необходимо заполнить их данными. Для этого используется SQL-инструкция INSERT, которая позволяет добавить записи в таблицы. Например, можно добавить информацию о блоках и транзакциях, которые являются основными элементами блокчейна.

В результате выполнения всех этих шагов будет создана база данных, которая соответствует требованиям блокчейна. База данных будет содержать необходимые таблицы с соответствующей структурой, а также заполнена актуальными данными. Создание базы данных является важным этапом разработки, поскольку она является основой для работы приложения и обеспечивает эффективное хранение и управление данными.

Таким образом, создание структуры базы данных позволяет эффективно организовать хранение информации о блоках и транзакциях, что является основой для функционирования блокчейна.

**3.2 Реализации логики работы блокчейна**

В данном разделе представлен процесс разработки программного кода, который обеспечивает стабильное и эффективное функционирование блокчейна, нод, криптографических модулей и веб-интерфейса. Основные технические детали и ключевые аспекты работы кода детально рассмотрены с целью выявления основных принципов его функционирования.

Описание каждого модуля происходит в логическом порядке, начиная с архитектурного обзора и перехода к более детальному рассмотрению каждого компонента. Особое внимание уделяется технологии синхронизации нод и их консенсуса, а также возможности автоматического мягкого форка, что представляет собой уникальную особенность разрабатываемого решения.

Помимо этого, в работе происходит анализ плюсов и уникальных особенностей применяемой технологии, а также рассматриваются потенциальные пути для ее дальнейшего развития и усовершенствования. Все это призвано создать полное и глубокое понимание работы и возможностей разработанного программного продукта.

**3.2.1 Архитектура**

Для эффективной установки всех необходимых пакетов проекта следует создать файл "requirements.txt", перечислив в нем все библиотеки и их версии, а затем воспользоваться инструментом pip для их установки. Этот подход значительно упрощает процесс управления зависимостями, позволяя легко обновлять библиотеки и гарантировать совместимость среды разработки.

Создание базовой структуры проекта важно для сохранения порядка и удобства работы. Подобная организация каталогов по модулям и функциональности помогает разработчикам легко найти нужные файлы и облегчает сопровождение кода. Каждый модуль может содержать свои собственные файлы, отвечающие за конкретные аспекты проекта, что способствует его более эффективной разработке и поддержке.

Итоговая архитектура проекта в файловой системе:

.

├── alembic.ini

├── chain

│   ├── \_\_init\_\_.py

│   ├── block.py

│   ├── constants.py

│   ├── db

│   │   ├── \_\_init\_\_.py

│   │   ├── base.py

│   │   ├── block.py

│   │   ├── session.py

│   │   └── transaction.py

│   ├── timestamps.py

│   └── transaction.py

├── chain\_config.py

├── crypto

│   ├── \_\_init\_\_.py

│   ├── bech32.py

│   ├── converter.py

│   ├── generate\_wallet.py

│   ├── poa\_mnemonic.py

│   ├── sign.py

│   └── transfer.py

├── migration

│   ├── README

│   ├── env.py

│   ├── script.py.mako

│   └── versions

│   ├── 004766e0c634\_.py

│   ├── 7477f995b497\_initial.py

│   ├── 81396b4c6d04\_.py

│   ├── 8da8420576da\_.py

│   ├── 9f31208dc33e\_.py

│   ├── dd7cc63002ed\_.py

│   ├── ee3fd4166e49\_.py

│   └── efc133a3c757\_.py

├── node

│   ├── \_\_init\_\_.py

│   ├── api

│   │   ├── \_\_init\_\_.py

│   │   ├── block.py

│   │   ├── distributor.py

│   │   ├── status.py

│   │   ├── transaction.py

│   │   └── user.py

│   ├── app.py

│   ├── blockchain

│   │   ├── \_\_init\_\_.py

│   │   ├── balancer.py

│   │   ├── block\_processing.py

│   │   ├── startup.py

│   │   └── validate.py

│   ├── models

│   │   ├── \_\_init\_\_.py

│   │   ├── block.py

│   │   └── transaction.py

│   ├── routers

│   │   ├── \_\_init\_\_.py

│   │   ├── alive.py

│   │   ├── block.py

│   │   ├── receive\_block.py

│   │   ├── receive\_transaction.py

│   │   ├── transactions.py

│   │   └── user.py

│   ├── structs

│   │   ├── \_\_init\_\_.py

│   │   └── block.py

│   └── utils.py

├── node\_constants.py

├── requirements.txt

├── run\_node\_gaz.sh

├── run\_node\_sber.sh

├── run\_node\_yandex.sh

├── run\_web.sh

└── web

├── \_\_init\_\_.py

├── app.py

├── constants.py

├── encryption.py

├── file\_response.py

├── models

│   ├── \_\_init\_\_.py

│   └── mnemonic.py

├── routers

│   ├── \_\_init\_\_.py

│   ├── address\_watcher.py

│   ├── blocks\_watcher.py

│   ├── index.py

│   ├── mnemonic.py

│   ├── sign.py

│   ├── transaction.py

│   └── wallet.py

├── static

│   ├── css

│   │   ├── index.css

│   │   └── wallet.css

│   ├── html

│   │   ├── address.html

│   │   ├── block.html

│   │   ├── blocks.html

│   │   ├── login.html

│   │   ├── transaction.html

│   │   └── wallet.html

│   ├── images

│   │   ├── favicon.ico

│   │   ├── logback.jpg

│   │   └── logo.png

│   └── js

│   ├── block.js

│   ├── blocks.js

│   ├── index.js

│   ├── transaction.js

│   └── wallet.js

└── utils.py

**3.2.2 Модуль блокчейна**

Модуль блокчейна отвечает за хранение, создание, обновление и удаление блоков и транзакций. А также рассчет хешей на основе внутренних данных блоков и транзакций.

Блоки в блокчейне являются основными элементами данных, которые хранят информацию о транзакциях, контрактах или других событиях. Они связаны между собой в цепочку, обеспечивая непрерывность и безопасность хранения данных. Каждый блок содержит ссылку на предыдущий блок и хеш, который обеспечивает целостность и невозможность изменения прошлых записей. Блоки позволяют всем участникам системы видеть историю изменений и подтверждать их подлинность, обеспечивая надежность и безопасность работы блокчейна.

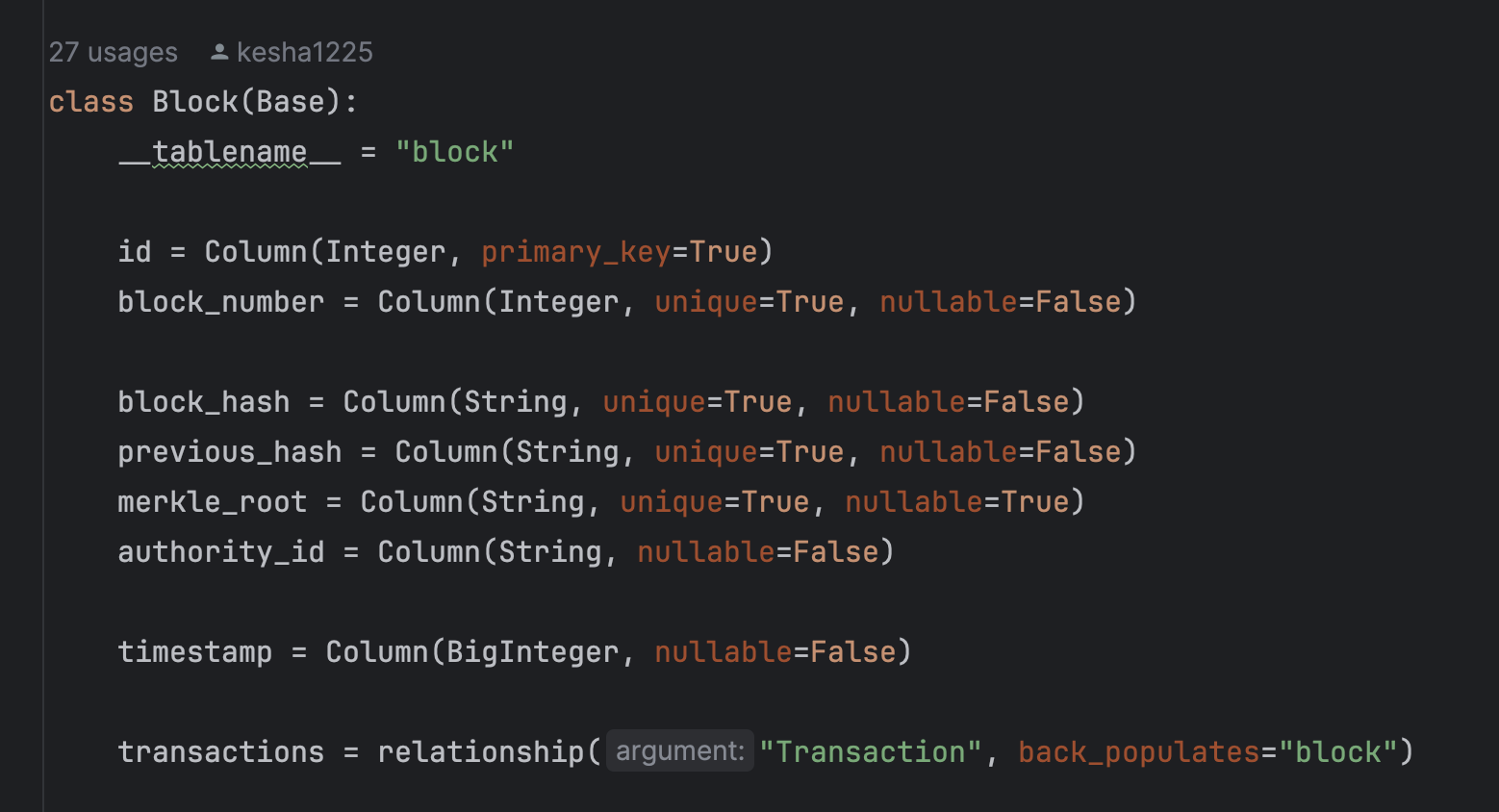


Рисунок 4 – структура блока в базе данных

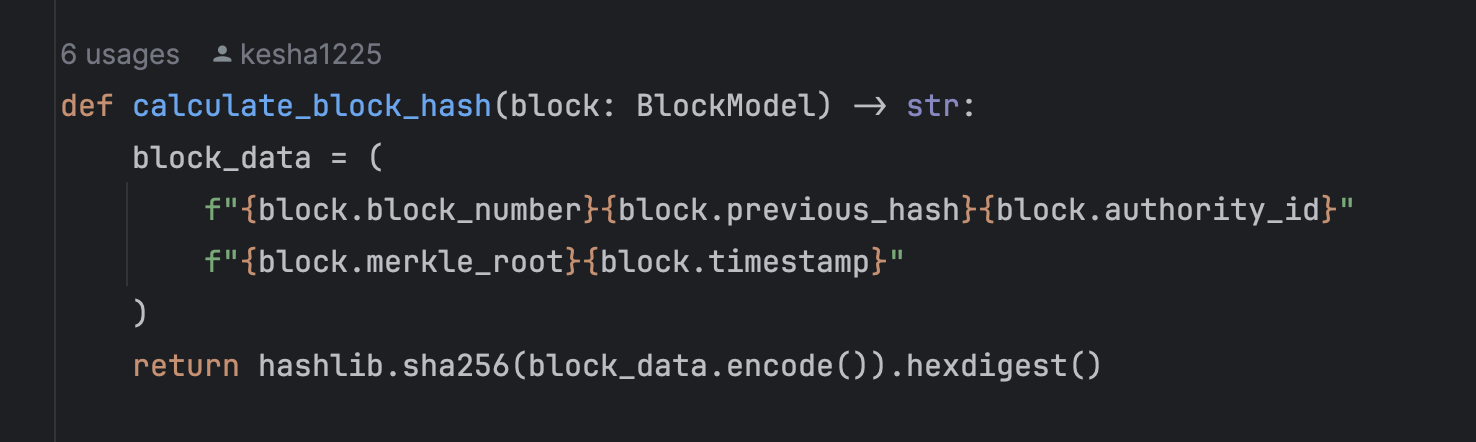


Рисунок 5 – функция рассчета хеша блока

Nonce (number used once) - это случайное число, используемое в процессе майнинга блоков в блокчейне Proof of Work (PoW). Он добавляется к блоку вместе с другими данными, чтобы изменить хеш блока и удовлетворить сложность доказательства работы (PoW). В блокчейне на PoW, майнеры должны перебирать различные значения nonce до тех пор, пока не найдут подходящий хеш блока.

В блокчейне на Proof of Authority (PoA) nonce не требуется, поскольку в этом типе консенсуса блоки создаются определенными авторизованными узлами, а не майнерами, конкурирующими за решение математической задачи. Необходимость в nonce отпадает, поскольку в PoA нет необходимости доказывать выполнение работы для создания блоков. Это позволяет упростить процесс формирования блоков и увеличить производительность сети, так как нет необходимости тратить ресурсы на вычисление подходящего nonce.

Отсутствие nonce в блокчейне на PoA можно считать важным улучшением, поскольку это уменьшает энергозатраты, связанные с процессом майнинга, и повышает эффективность сети блокчейна. Благодаря этому блокчейн на PoA становится более экологически чистым и масштабируемым, что важно для его долгосрочной устойчивости и развития.

Отсутствие лимита на количество транзакций в блокчейне является важным преимуществом и отличием от других блокчейнов, таких как биткоин и другие медленные криптовалюты. Вот несколько причин, почему это так:

Высокая пропускная способность: Блокчейн без ограничения на количество транзакций в блоке может обрабатывать больше транзакций за тот же период времени, что увеличивает общую пропускную способность сети. Это позволяет ускорить время подтверждения транзакций и обеспечить более быстрый оборот средств.

Отсутствие комиссий: Поскольку блоки могут вмещать больше транзакций, конкуренция за включение транзакций в блок становится менее острой. Это позволяет убрать комиссии за транзакции для пользователей, что делает использование блокчейна более доступным и экономически выгодным.

Улучшенная масштабируемость: Отсутствие ограничений на количество транзакций в блоке способствует улучшению масштабируемости блокчейна. Блокчейны с высокой пропускной способностью могут эффективно обслуживать большое количество пользователей и транзакций без существенного снижения производительности.

Улучшенный пользовательский опыт: Более быстрые и дешевые транзакции делают использование блокчейна более удобным для пользователей, улучшая общий пользовательский опыт и привлекательность платформы.

Таким образом, отсутствие лимита на количество транзакций в блоке способствует повышению эффективности и производительности блокчейна, что делает его более конкурентоспособным и привлекательным для пользователей.

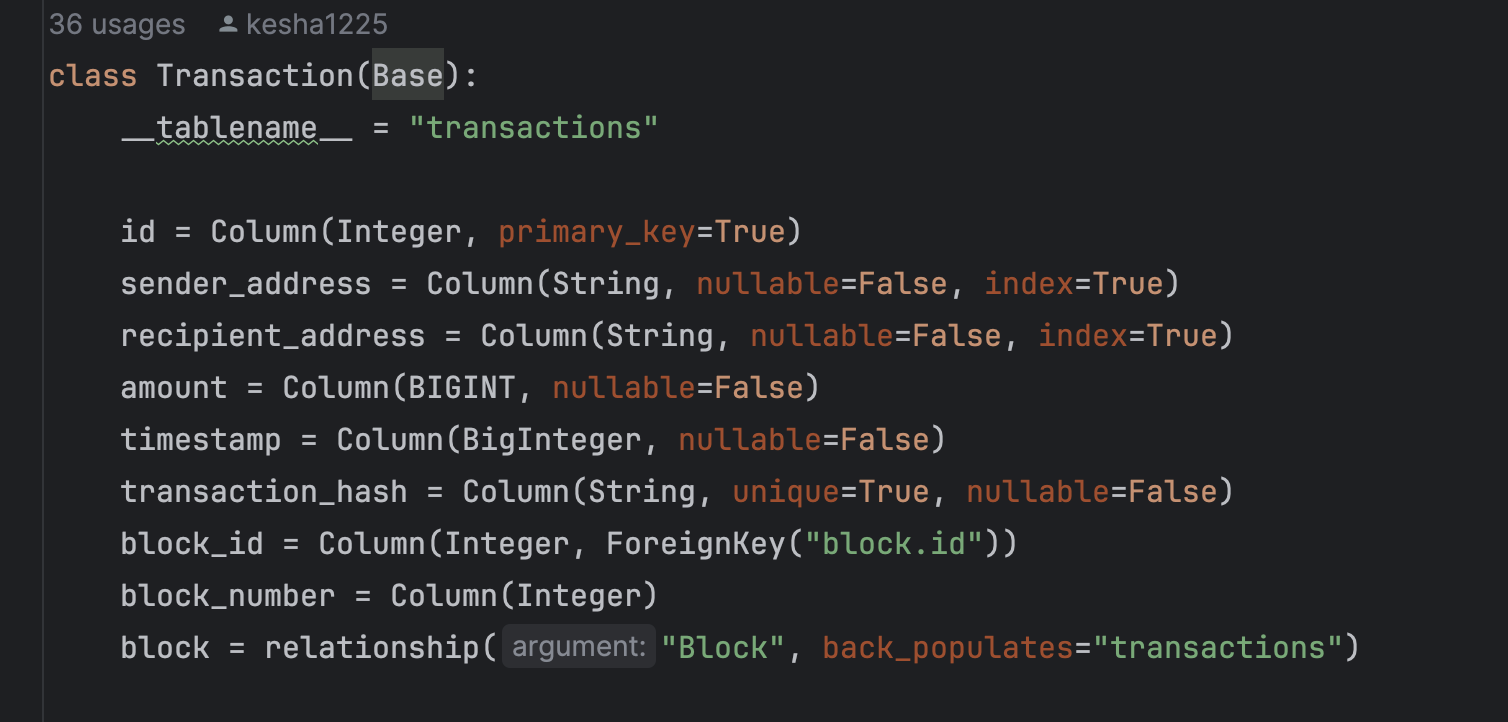


Рисунок 6 – структура транзакции в базе данных

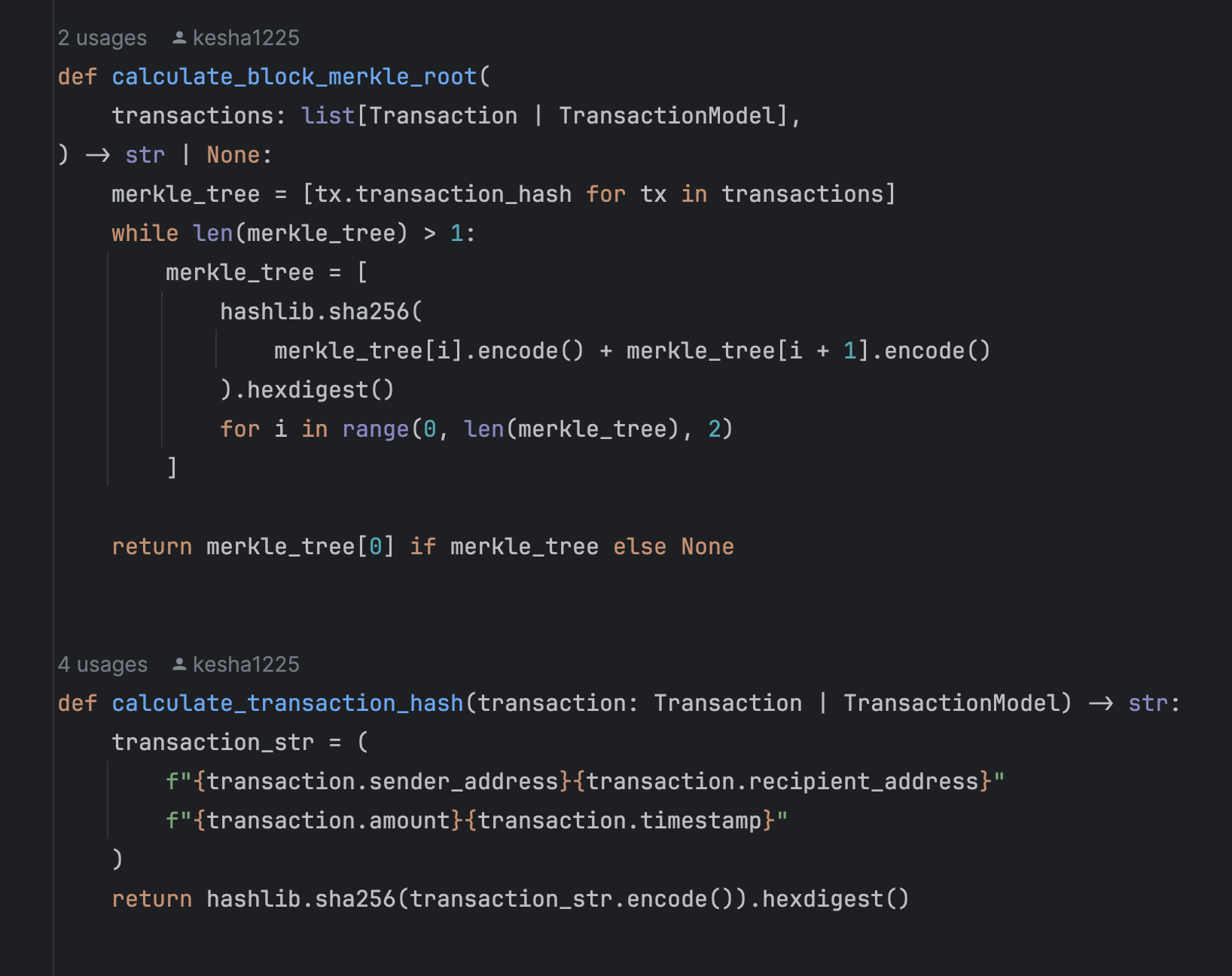


Рисунок 7 – Функции вычисления дерева меркла и хеша транзакции

Добавление случайного числа в транзакции блокчейна используется для предотвращения возникновения одинаковых хешей в случае, если две или более транзакции имеют одинаковые параметры. Это делает атаки на блокчейн сложнее, так как даже небольшие изменения в транзакции приведут к различным хешам блоков.

Однако, в этом случае я использовал более точное время до микросекунд вместо случайного числа, чтобы обеспечить уникальность хеша транзакции. Это значит, что каждая транзакция будет иметь уникальное время создания, которое до микросекунд точно отражает момент создания транзакции. Поскольку время до микросекунд является уникальным для каждой транзакции, нет необходимости в использовании случайного числа для предотвращения коллизий хешей.

Использование точного времени до микросекунд вместо случайного числа позволяет избежать хранения дополнительных данных в транзакциях и сделать их более легкими и эффективными. Такой подход также обеспечивает безопасность и уникальность каждой транзакции без необходимости генерации случайных чисел.

В базе данных для хранения блоков и транзакций использование индексов на полях sender\_address и recipient\_address является полезным с точки зрения оптимизации производительности и ускорения выполнения запросов. Индексы на эти поля позволяют значительно снизить время выполнения запросов, связанных с поиском или фильтрацией транзакций по отправителю или получателю.

Использование индексов на полях sender\_address и recipient\_address позволяет базе данных эффективно находить все транзакции, отправленные или полученные конкретным адресом. Это особенно полезно при выполнении запросов на поиск истории транзакций для определенного адреса или при анализе транзакций между определенными адресами.

Благодаря индексам на указанных полях база данных может быстро определить, какие записи соответствуют критериям запроса, что уменьшает время ответа и улучшает общую производительность системы. Такое оптимизированное хранение и доступ к данным важно для эффективной работы блокчейна, особенно при обработке большого объема транзакций.

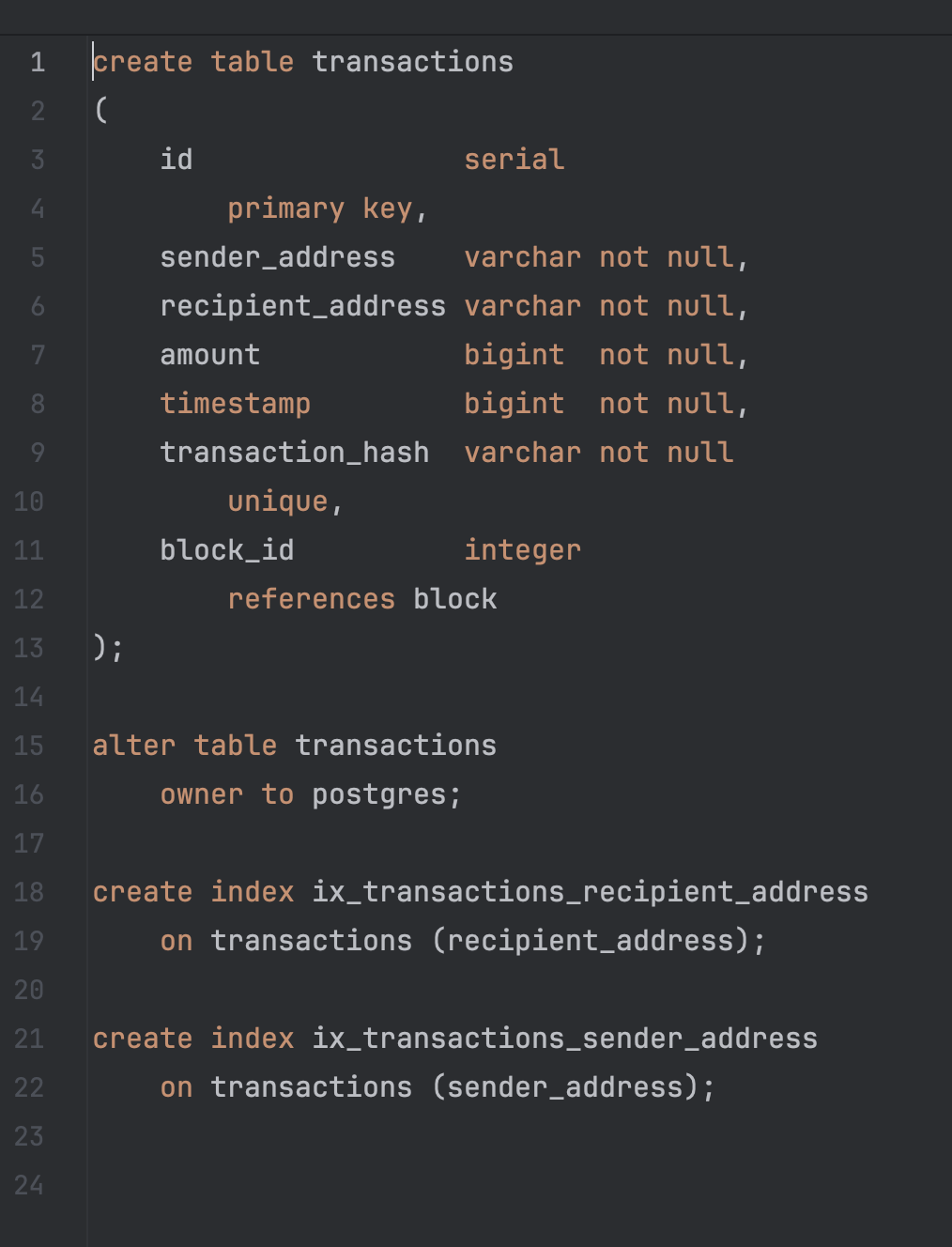


Рисунок 8 – Описание модели транзакции на DDL вместе с индексами на полях sender\_address и recipient\_address

Bech32 - это формат адресов, используемый в блокчейне, который представляет собой надежный и эффективный способ кодирования данных. Он основан на алгоритме Безье, который обеспечивает высокую степень надежности и устойчивости к ошибкам при передаче данных.

Одним из ключевых преимуществ Bech32 является его способность предотвращать ошибки при копировании и вводе адресов. Это достигается за счет использования символов, которые легко различимы человеческим глазом и имеют высокую степень различимости между собой. Это делает Bech32 идеальным выбором для блокчейна на PoA, где точность и надежность важны для успешной обработки транзакций.

Кроме того, Bech32 обеспечивает эффективное использование места и уменьшает размер передаваемых данных. Это особенно важно для блокчейна на PoA, где меньший размер транзакций приводит к более быстрой обработке и уменьшает нагрузку на сеть.

Таким образом, Bech32 является идеальным выбором для блокчейна на PoA благодаря своей высокой надежности, эффективному использованию места и способности предотвращать ошибки при передаче данных.

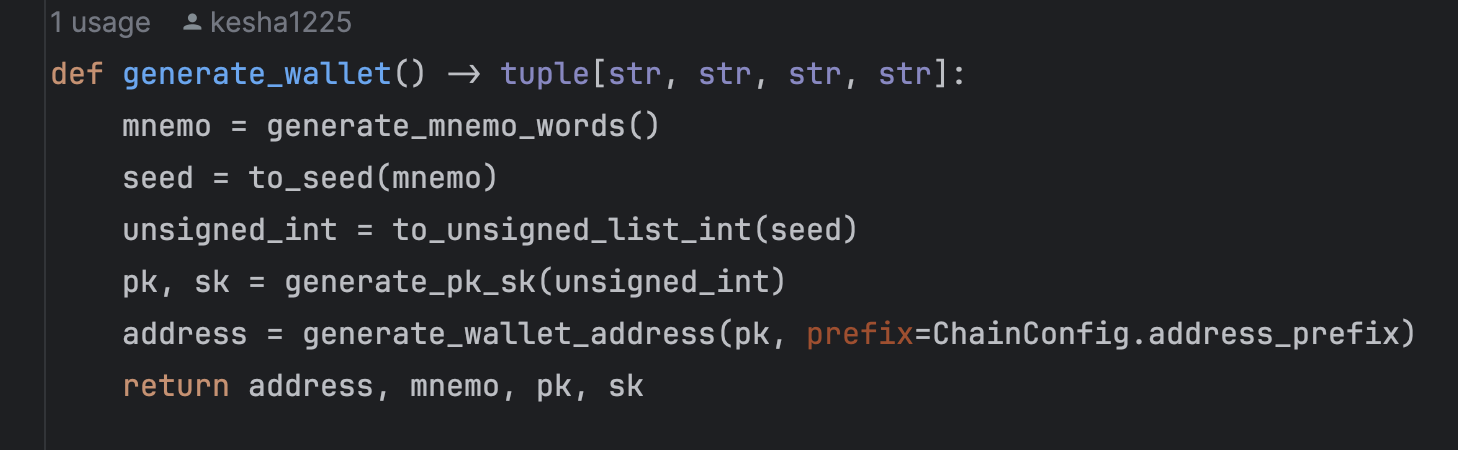


Рисунок 9 – функция генерации кошелька с префиксом poa с помощью bech32

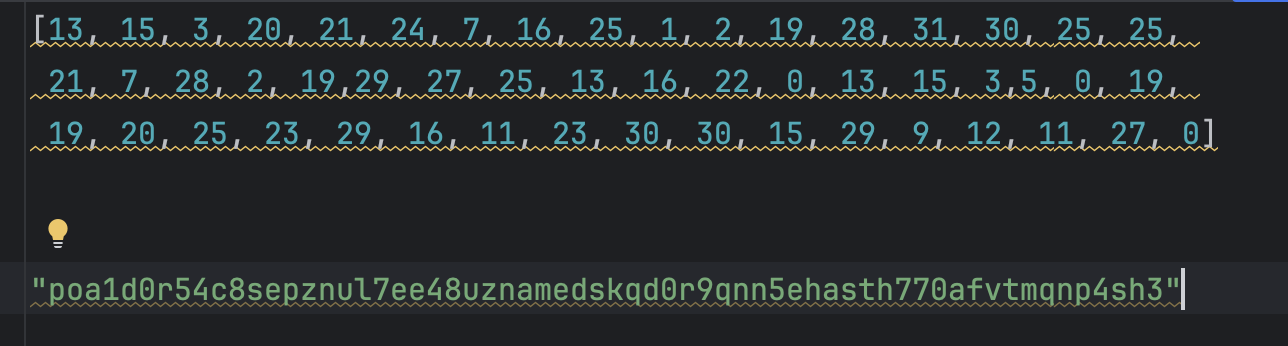


Рисунок 10 – Конвертированные байты из публичного ключа и адрес получившийся из них путем закодирования с помощью bech32

Описание модуля блокчейна, представленное выше, подчеркивает ключевые аспекты его разработки и функционирования. Рассмотрены основные компоненты блокчейна, включая структуру блока, транзакции, ноды и веб-интерфейс. Архитектура проекта основана на использовании СУБД PostgreSQL, клиентского веб-интерфейса и нод, что обеспечивает надежную и эффективную работу блокчейна.

Использование инновационных технологий, таких как Bech32 для адресации и точное время до микросекунд для обеспечения уникальности транзакций, подчеркивает стремление к оптимизации и улучшению производительности блокчейна. Такой подход отражает не только технический аспект проекта, но и его стремление к созданию надежной и эффективной системы для проведения трансграничных транзакций.

**3.2.3 Модуль ноды**

Модуль ноды – это сердце блокчейна. Он отвечает за создание, проверку и утверждение блоков, которые составляют основу цепи транзакций. Этот модуль также обеспечивает взаимодействие пользователей с блокчейном через веб-интерфейс.

Нода является ключевым элементом сети, так как именно здесь происходит процесс генерации новых блоков на основе подтвержденных транзакций. Кроме того, нода отвечает за поддержание согласованности и безопасности сети блокчейна.

Особенностью этого модуля является его распределенность. Ноды блокчейна могут быть развернуты в различных местах сети, что обеспечивает децентрализацию и надежность системы. Также нода способна взаимодействовать с другими узлами блокчейна для синхронизации данных и подтверждения блоков.

Таким образом, модуль ноды играет ключевую роль в функционировании блокчейна, обеспечивая его работу и взаимодействие с пользовательскими интерфейсами.

От владельца для запуска нода требует 4 секретных параметра:

- POSTGRES\_URL: Ссылка на базу данных

- POSTGRES\_URL\_ALEMBIC: Ссылка на базу данных для миграции

- NODE\_ID: Уникальный ключ-название ноды  
- PRIVATE\_KEY: Секретный ключ для подписывания блоков

При запуске нода автоматически мигрирует возможные обновления в базе и начинает процесс предзапуска.

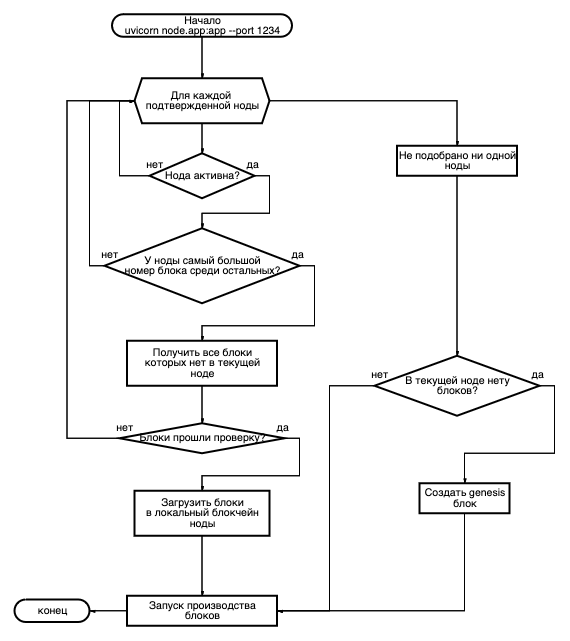


Рисунок 11 – Блок схема описывающая процесс запуска ноды до момента запуска производства блоков

После запуска и синхронизации нода переходит к процессу которым она и будет заниматься весь свой жизненный цикл – производству блоков.

Описание процесса производства блоков и управления статусами нод очень информативное. Описание процесса шаг за шагом:

Производство блоков: Ноды производят блоки с заданной периодичностью (например, каждые 10 секунд). Этот интервал времени выбирается для предотвращения переизбытка данных блоков с пустыми транзакциями и для накопления транзакций для обработки.

Статусы нод: У нод есть два основных статуса - "готовность" и "ожидание". При запуске нода находится в статусе "ожидание". Если нет других активных нод, то нода становится "готовой", иначе она остается в режиме ожидания.

Создание блока: Когда наступает время для создания блока, активная и готовая нода берет все неподтвержденные транзакции, созданные через нее, и формирует новый блок, вычисляя дерево Меркла на основе этих транзакций.

Рассылка уведомлений: Нода отправляет уведомление всем другим активным нодам о предстоящем выпуске нового блока, подписывая его собственным ключом.

Проверка уведомлений: Активные ноды получают уведомление, проверяют его подпись и отклоняют, если подпись неверна. Если проверка прошла успешно, они переходят к следующему шагу.

Добавление блока в блокчейн: Блок добавляется в локальную копию блокчейна текущей ноды, и в него включаются данные о новом блоке и его транзакциях.

Рассылка блока: Новый блок рассылается всем остальным активным нодам с подписью.

Прием блока другими нодами: Другие активные ноды принимают блок, валидируют его подпись и хеши всех транзакций.

Переход к следующей ноде: Очередь переключается на следующую ноду по порядку, и весь процесс повторяется.

Этот процесс позволяет поддерживать целостность и консистентность блокчейна, а также обеспечивает равномерное распределение обязанностей между нодами в сети.

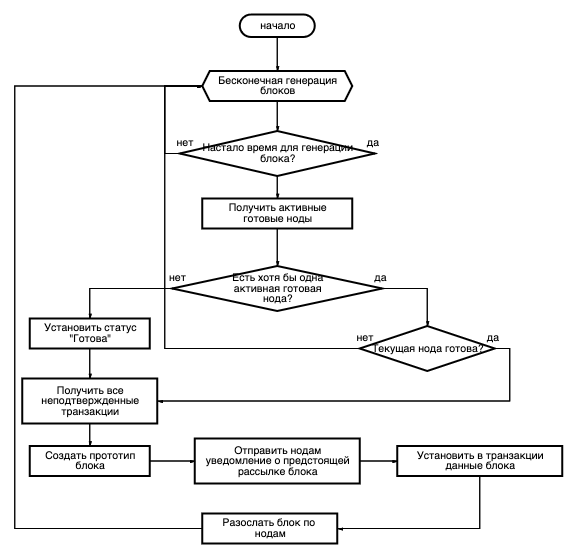


Рисунок 12 – Блок схема описывающая генерацию блоков нодой.

Модуль ноды является центральным элементом блокчейна, ответственным за создание, проверку и утверждение блоков, а также за взаимодействие с пользовательскими интерфейсами через веб-интерфейс. Он играет ключевую роль в функционировании блокчейна, обеспечивая его работу и безопасность.

Особенностью этого модуля является его децентрализованность: ноды блокчейна могут быть развернуты в различных местах сети, что обеспечивает надежность и согласованность системы. Ноды также взаимодействуют между собой для синхронизации данных и подтверждения блоков.

Процесс производства блоков подразумевает создание новых блоков с определенной периодичностью, а также управление статусами нод для обеспечения равномерного распределения обязанностей между ними. Этот процесс позволяет поддерживать целостность и консистентность блокчейна.

Таким образом, модуль ноды является ключевым элементом блокчейна, обеспечивающим его нормальную работу и взаимодействие с внешними интерфейсами.

**3.2.4 Модуль веб-интерфейса**

Модуль веб интерфейса